PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-093548
(43)Date of publication of application : 10.04.1998

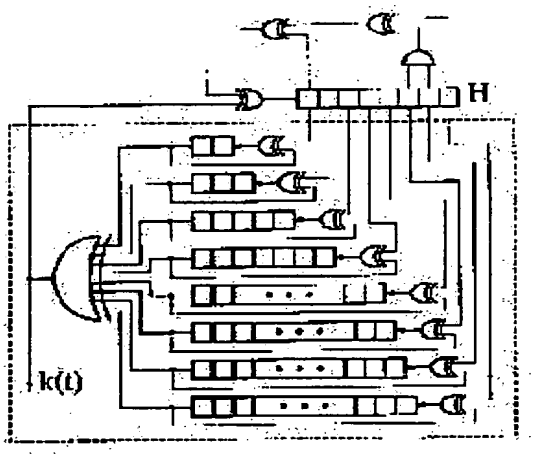
(51)Int.Cl. H04L 9/24
G09C 1/00
G09C 1/00

(21)Application number : 08-245158
(22)Date of filing : 17.09.1996

(71)Applicant : AIONIKUSU OKINAWA KK
(72)Inventor : KIYATAKE MORIMOTO
OKINAGA KENJI
NAKAMURA MORIKAZU

(54) PSEUDO RANDOM BIT STREAM GENERATOR AND CIPHERING COMMUNICATION METHOD USING THE SAME

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a pseudo random bit generator with improved security and a simple circuit configuration of a pseudo random bit generator employing a plurality of FSRs by providing a means that feeds back an output of an exclusive OR means to a plurality of feedback shift registers(FSRs).
SOLUTION: A circuit shown in dashed lines is inputted with an exclusive OR so that a seed (secret key) is dynamically changed in a basic pseudo random bit sequence generator. This input is generated by a register H of a nonlinear auxiliary circuit. The register H is added to the basic pseudo random bit stream generator where contents of each FSR are dynamically changed for each circuit operation to configure a dynamic basic pseudo random bit sequence generator. At first, the Seed is inputted to each FSR and an auxiliary circuit and data are shifted one by one bit sequentially while synchronizing a shift clock with a communication speed. The register H sends data to each FSR to change the Seed dynamically. Then exclusive OR processing is applied to an output from each FSR.



LEGAL STATUS

[Date of request for examination]	06.01.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3358954
[Date of registration]	11.10.2002
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－93548

(43)公開日　平成10年(1998)４月10日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/24		Ｈ０４Ｌ	9/00	６５７
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ	1/00	６１０Ｄ
		６５０			６５０Ｂ

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）

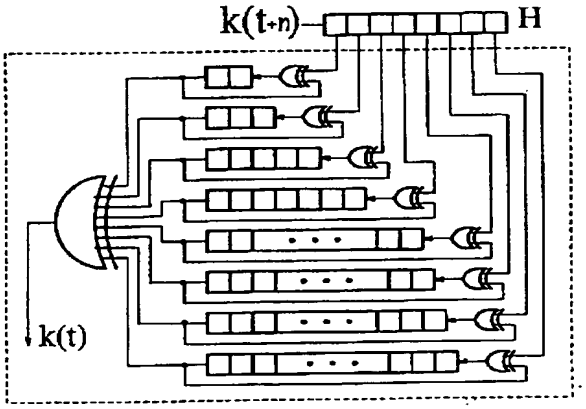
(21)出願番号　特願平8－245158

(22)出願日　平成８年(1996)９月17日

(71)出願人　596136006
アイオニクス沖縄株式会社
沖縄県浦添市西洲２丁目２番地３
(72)発明者　喜屋武　盛基
沖縄県沖縄市首里汀良町３－63－１
(72)発明者　翁長　健治
沖縄県那覇市上之屋409－12
(72)発明者　名嘉村　盛和
沖縄県宜野湾赤道２－14－６　仲アパートＢ－５室
(74)代理人　弁理士　大塚　康徳　（外２名）

(54)【発明の名称】　擬似ランダムビット列生成器及びそれを使用する暗号通信方法

(57)【要約】
【課題】　従来の複数のフィードバックレジスタを用いた擬似ランダムビット列生成器の欠点であった短い周期性を改善しながら、複数のフィードバックレジスタを用いた擬似ランダムビット列生成器の簡素な回路構成と安全性の尊重を目的とした、擬似ランダムビット列生成器及びそれを使用する暗号通信方法を提供する。
【解決手段】　互いに素数の長さを持つ複数のフィードバックシフトレジスタ（２ビット，３ビット，…）と、複数のフィードバックシフトレジスタの出力の排他的論理和をとる排他的論理和回路と、排他的論理和回路の出力を複数のフィードバックシフトレジスタにフィードバックするフィードバック回路Ｈとを備え、最初の予備Ｓｅｅｄをセットして本Ｓｅｅｄを作成することで、本Ｓｅｅｄのランダム性を高め、且つ送信側から受信側へ送信するＳｅｅｄデータを少なくする。



1

【特許請求の範囲】

【請求項１】　ランダムビット列を使用する暗号通信において使用される擬似ランダムビット列生成器であって、

互いに素の長さを持つ複数のフィードバックシフトレジスタと、

該複数のフィードバックシフトレジスタの出力の排他的論理和をとる排他的論理和手段と、

該排他的論理和手段の出力を前記複数のフィードバックシフトレジスタにフィードバックするフィードバック手段とを備えることを特徴とする擬似ランダムビット列生成器。

【請求項２】　前記複数のフィードバックシフトレジスタを選択する選択手段を更に備え、

前記排他的論理和手段は、選択されたフィードバックシフトレジスタの出力の排他的論理和をとることを特徴とする請求項１記載の擬似ランダムビット列生成器。

【請求項３】　前記フィードバック手段は、前記排他的論理和手段の出力に対応して前記複数のフィードバックシフトレジスタのフィードバック値を変更するフィードバック変更手段を更に備えることを特徴とする請求項１または２記載の擬似ランダムビット列生成器。

【請求項４】　擬似ランダムビット列生成器を使用する暗号通信方法であって、

前記擬似ランダムビット列生成器が、互いに素の長さを持つ複数のフィードバックシフトレジスタと、該複数のフィードバックシフトレジスタを選択する選択手段と、選択されたフィードバックシフトレジスタの出力の排他的論理和をとる排他的論理和手段と、該排他的論理和手段の出力を前記複数のフィードバックシフトレジスタにフィードバックするフィードバック手段とを備え、

送信側では、選択されるフィードバックシフトレジスタの初期データを受信側で復号されるデータに変換し、前記初期データを用いた前記擬似ランダムビット列生成器で暗号化して受信側に送り、

受信側では、受信データを以前の初期データを使用して前記選択されるフィードバックシフトレジスタを使用して復号し、復号されたデータを新たな前記複数のフィードバックシフトレジスタの初期データとして以降の受信データを復号することを特徴とする暗号通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は擬似ランダムビット列生成器、特に暗号通信に使用される擬似ランダムビット列生成器及びそれを使用する暗号通信方法に関するものである。

【０００２】

【従来の技術】情報化社会が発達した現代、データ通信を行なう際には、情報を安全に運用する技術すなわち情報セキュリティ技術の重要性が増してきている。特に、

2

データ秘匿に関する暗号は、その実現や解読等種々の研究が行なわれている。秘匿性を伴うデータ通信や最近発展のめざましい通信ネットワークにおける回線暗号装置では、一般にストリーム暗号が用いられており、ＩＳＯの国際規格ＩＳ－９１６０（物理レイヤ暗号装置に対する相互運用要求事項）においても、回線暗号装置で用いる暗号としては、１ビットまたは８ビット（１文字）ごとのストリーム暗号を使うように規定している。

【０００３】ストリーム暗号の一種としてバーナム暗号法があるが、この方式は原理が簡単で且つキーストリームが使い捨てなため、安全性の高い暗号法として良く用いられている。この暗号法の一番の関心事は、キーストリームを如何にして生成するかであるが、これに真の物理的ランダムビット列を用いた場合には理論的に解析が不可能な唯一の暗号となる。しかし、一般にバーナム暗号法では、通信文と同じ量だけのキーストリームを別の送信先に送ることは非現実的であることから、乱数として真の物理的ランダムビット列は用いずに比較的簡単な方法で生成した擬似ランダムビット列を用いる。従って、この擬似ランダムビット列の性質が、暗号の強度を大きく左右することになる。

【０００４】擬似ランダムビット列生成には、比較的短い秘密鍵（７０ビット程度）から長い擬似ランダムビット列を生成する必要があるが、その手段として従来、

１．線形フィードバックシフトレジスタ（Linear Feedback Shift Register：ＬＦＳＲ）を組み合わせた方法

２．ＤＥＳ（Data Encrtption Standard：ＤＥＳ）暗号装置等を用いる方法

３．ＬＦＳＲと論理素子を組み合わせた非線形結合による方法

４．クロック制御型の擬似ランダクビット系列生成器（Clock-Controlled Generator：ＣＣＧ）を用いる方法

等が用いられてきた。

【０００５】

【発明が解決しようとする課題】しかしながら、１．は良好な擬似ランダクビット列をもつＭ系列（Maximum-length linear feedback shift register sequence：最大周期系列）が含まれるが暗号用擬似ランダクビット列としてみれば安全性は弱く、レジスタのステージ数をｎとした場合、わずか２ｎの既知平文とそれに対応する暗号文があれば秘密鍵であるレジスタの初期値とタップ列が解析的に解読されてしまう（既知平文攻撃）。また、

２．は別の暗号アルゴリズムとして設計されたブロック暗号方式の暗号法であるが、出力の一部をキーストリームとすることにより擬似ランダムビット列生成器に適用できる。しかし、アルゴリズムが複雑で多数の換字，置換による構成のため解析的攻撃に強いが回路が複雑になる。また、３．は製造仕様が非公開であるので量産が困難であり、たとえ公開型であるとしても、高次の非線形結合を得るために秘密鍵（Seed）が大きくなる等の欠点

がある。

【０００６】そこで、これらの欠点を補うために、複数のフィードバックレジスタを用いた擬似ランダムビット列生成器の研究が行われている。この擬似ランダムビット列生成器はＳｅｅｄの数が少なく、簡単な構成により安全性の比較的高い乱数系列が得られる特徴を持つ。しかし、系列のランダム性は持ち得るが、短い周期を有するので最近の画像データ等の大きなデータ通信には対応できなくなってきた。

【０００７】本発明は、従来の複数のフィードバックレジスタを用いた擬似ランダムビット列生成器の欠点であった短い周期性を改善しながら、複数のフィードバックレジスタを用いた擬似ランダムビット列生成器の簡素な回路構成と安全性の尊重を目的とした、擬似ランダムビット列生成器及びそれを使用する暗号通信方法を提供する。

【０００８】

【課題を解決するための手段】この課題を解決するために、本発明の擬似ランダムビット列生成器は、ランダムビット列を使用する暗号通信において使用される擬似ランダムビット列生成器であって、互いに素の長さを持つ複数のフィードバックシフトレジスタと、該複数のフィードバックシフトレジスタの出力の排他的論理和をとる排他的論理和手段と、該排他的論理和手段の出力を前記複数のフィードバックシフトレジスタにフィードバックするフィードバック手段とを備えることを特徴とする。

【０００９】ここで、前記複数のフィードバックシフトレジスタを選択する選択手段を更に備え、前記排他的論理和手段は、選択されたフィードバックシフトレジスタの出力の排他的論理和をとる。また、前記フィードバック手段は、前記排他的論理和手段の出力に対応して前記複数のフィードバックシフトレジスタのフィードバック値を変更するフィードバック変更手段を更に備える。

【００１０】又、本発明の暗号通信方法は、擬似ランダムビット列生成器を使用する暗号通信方法であって、前＊記擬似ランダムビット列生成器が、互いに素の長さを持つ複数のフィードバックシフトレジスタと、該複数のフィードバックシフトレジスタを選択する選択手段と、選択されたフィードバックシフトレジスタの出力の排他的論理和をとる排他的論理和手段と、該排他的論理和手段の出力を前記複数のフィードバックシフトレジスタにフィードバックするフィードバック手段とを備え、送信側では、選択されるフィードバックシフトレジスタの初期データを受信側で復号されるデータに変換し、前記初期データを用いた前記擬似ランダムビット列生成器で暗号化して受信側に送り、受信側では、受信データを以前の初期データを使用して前記選択されるフィードバックシフトレジスタを使用して復号し、復号されたデータを新たな前記複数のフィードバックシフトレジスタの初期データとして以降の受信データを復号することを特徴とする。

$$K[t] = r_2[t] (+) r_3[t] (+) r_5[t] (+) \cdots (+) r_{17}[t] (+) r_{19}[t]$$

と表せる。

【００１４】上記基本擬似ランダムビット列生成器は、回路構成がＦＳＲと排他的論理和により結合した回路なので、出力される系列は一定の値を最大値とする周期を持つ。各段のＦＳＲが素の長さのために、各ＦＳＲから※

$$S = 2\times3\times5\times7\times11\times13\times17\times19 = 9699690 \fallingdotseq 10^7 \quad \cdots (2)$$

＜周期性の改善例＞上記図１の基本擬似ランダムビット列生成器は、Ｓｅｅｄの並びが静的で、その回路構成のために周期が短い。そこで、暗号用乱数としての安全性を保ちながらも、周期を伸ばす方法として、回路動作時にＳｅｅｄを動的に変化させ、長周期化の実現を図る。提案する回路を図２に示す。尚、回路内部は公開とする。

【００１１】

【発明の実施の形態】

＜本実施の形態の擬似ランダムビット列生成器の原理＞

図１に、複数のフィードバックレジスタを用いた擬似ランダムビット列生成器の基本回路構成例を示す。

【００１２】図１では、擬似ランダムビット列生成器として適当なレジスタ数として、例えば２～１９の素の長さの８つのフィードバックシフトレジスタ(Feedback Sift Register：ＦＳＲ）を用い、ＦＳＲの出力を排他的論理和結合とする。動作原理としては、まず各段のＦＳＲに初期値として種（Ｓｅｅｄ）を入力する。Ｓｅｅｄのサイズは２＋３＋５＋…＋１７＋１９＝７７ビットである。通信の際に、各段のＦＳＲをシフトさせると各段の左端から‘0’か‘1’が出力され、排他的論理和回路でこれら出力の排他的論理和を取った出力が、得られる擬似ランダムビット列となる。

【００１３】この回路の出力Ｋ［ｔ］は、各レジスタのｔステップ時の出力を$r_2[t]$，$r_3[t]$，$r_5[t]$，…，$r_{17}[t]$，$r_{19}[t]$とした場合、

※の出力が程よく組み合わされて効率よい周期が得られる特徴を持ち、最大周期Ｓは各段のＦＳＲのビット数の積により式（２）で表すことができる。

【００１５】

る。

【００１６】波線部内の回路は、基本擬似ランダムビット列生成器にＳｅｅｄが動的に変化するよう排他的論理和の入力がなされている。この入力は、非線形を持つ補助回路のレジスタＨにより生成されている。回路動作毎に各ＦＳＲの中身が動的に変化することから、波線部内

の回路を基本擬似ランダムビット列生成器と称することとし、これに補助回路Ｈを付加して動的な擬似ランダムビット列生成器を構成する。この補助回路Ｈは、ＣＣＧでいう制御ＦＳＲにあたり、基本擬似ランダムビット列生成器内のＳｅｅｄを動的に変化させる働きをする。そのため、従来の出力系列を操作するＣＣＧではなく、Ｓｅｅｄの中身を制御する新しい型のＣＣＧと言える。

【００１７】動作原理としては、まずＤＮＳ回路の各ＦＳＲと補助回路内にＳｅｅｄを入力し、通信速度にシフトクロックを同期させながら順次１ビットずつシフトさせる。補助回路ＨはＤＮＳ回路内の各ＦＳＲにデータを送ることにより、Ｓｅｅｄを動的に変化させる役割を持つ。ＤＮＳ回路内各ＦＳＲからの出力に排他的論理和を施し、その出力が得られる擬似ランダムビット列となる。

【００１８】＜秘匿性の改善例１＞上記擬似ランダムビット列生成器を使用した暗号通信では、初期の全Ｓｅｅｄを送信側から受信側に送る必要があるため、例えＳｅｅｄを暗号化して送ったとしても、複雑な暗号化は伝送効率を低めるので簡単な暗号化となり、一旦Ｓｅｅｄが解読されると、暗号文の秘匿性が著しく低下する。また、Ｓｅｅｄを送らずに送信側と受信側とで同じＳｅｅｄを用意するようにしても、やはり暗号文の秘匿性が著しく低下する。

【００１９】図３は、上記秘匿性の低下を防ぎ、秘匿性の改善をした擬似ランダムビット列生成器の一例である。図３では、簡単な（例えばＳｅｅｄのビット長以上の周期のある）予備Ｓｅｅｄから全Ｓｅｅｄビットを作成するようにして、予備Ｓｅｅｄのみを送信側から受信側に送るようにした例である。例えば、全Ｓｅｅｄは７７ビットであるので、予備Ｓｅｅｄは３ビット，５ビット，７ビットのデータのみで、３×５×７＝１０５ビットの周期となり、全Ｓｅｅｄビットを疑似乱数として選ぶことが可能である。

【００２０】＜秘匿性の改善例２＞図４は、秘匿性の低下を防ぎ、秘匿性の改善をした擬似ランダムビット列生成器の他例である。図４の構成においては、図３のような予備Ｓｅｅｄの作成のみでなく、補助回路ＨによりＦＳＲを選択することで、図３と同様の全Ｓｅｅｄビットを作成する。又、この選択データ（補助回路Ｈにセットしたデータ）を暗号化して送信側から受信側に送るようにしてもよい。

【００２１】このようにすれば、上記例では選択データは８ビットであるので、複雑な暗号化を行っても伝送効率を低めることはない。又、通信毎に擬似ランダムビット列生成が変化するので、攻撃に対しても強い。尚、本例の場合は、ＦＳＲを２ビットから１９ビットの８つでなく、更に増加するのが好ましい。又、補助回路Ｈはシフトレジスタであっても良い。

＊【００２２】尚、図２，図３及び図４の回路は複合されても使用される。

＜暗号通信システムの構成及び動作例＞秘密鍵暗号方式として代表的なＤＥＳ暗号やＦＥＡＬ暗号(Fast Data Encipherment Algorithm)、或いは公開鍵暗号方式のほとんどがブロック単位に暗号／複号化される、いわゆるブロック暗号方式(block cipher)に属している。それに対して、ストリーム暗号(stream cipher) と呼ばれるクラシカルな方式が存在する。上記複数のフィードバックレジスタを用いた擬似ランダムビット列生成器はブロック暗号方式に適用されても効果を挙げるが、本例では特の効果の著しいバーナム暗号法というストリーム暗号の一種に適用した例を示す。

【００２３】ストリーム暗号とは、平文１ビット（或いは数ビット）とキーストリーム（出力鍵系列）の１ビット（数ビット）から暗号系列１ビット（或いは数ビット）が生成され、ブロック暗号のようにブロック単位で暗号／複号化されるのではなく、ビット単位で暗号／複号化処理がなされる。このキーストリーム発生に真の物理的ランダムビット列を用いた場合、理論的に解析が不可能な唯一の暗号となる。

【００２４】ストリーム暗号に属する暗号法の１つにバーナム暗号法(Vernam chipher)が存在する。バーナム暗号法は、キーストリームを使い捨てとすることにより暗号強度を高めている。このキーストリームに真の物理的ランダムビット列を用いた場合、理論的に解析が不可能な唯一の暗号となる。しかしバーナム暗号法では、通信文と同量のキーストリームを送信先に送信することは非現実的なため、真の物理的ランダムビット列は用いず、一般に比較的簡単な方法により生成した擬似ランダムビット列を用いる。従って、この擬似ランダムビット列の性質が暗号システム全体の強度を大きく左右することになり、最近では種々の擬似ランダムビット列生成器の提案、解読研究が進められている。

【００２５】バーナム暗号法は、１９１７年に電信用暗号として開発されたストリーム暗号の一種で、通信ネットワークにおける秘匿通信によく用いられている。換字暗号暗号（平文を他の文字等に変換する暗号）の鍵を十分に長い擬似ランダムビット列とすると無条件に完全な暗号を構成できることから、送信者側で平文（通信文）をキーストリーム（乱数鍵）で１ビットずつ論理演算を施して暗号化し、受信者側で暗号文を同じ鍵で複号化するものである。また、この擬似ランダムビット列による論理演算を通信速度と同期させることにより、暗号／複号化時間を無視することができ、高速なデータ通信が行える利点を持つ。このシステムの構成を図５に示す。

【００２６】平文のビット系列をＭ＝m_1 m_2 …とし、鍵のビット系列をｋ＝k_1 k_2 …とすると、暗号文のビット系列Ｃ＝c_1 c_2 …は、

$$c_i = (m_i + k_i) \bmod 2 \quad (i = 1, 2, \cdots) \quad \cdots (3)$$

となる。ｍｏｄでの和は排他的論理和のことからであるから、(+) を用いて、上式は、

$c_i = m_i(+)k_i$　　…（４）

と表される。復号化は同じ鍵を用いて、

$m_i = c_i(+)k_i$

$= m_i(+)k_i(+)k_i$

$= m_i$　　…（５）

となる。（ここで、k_i が‘０’，‘１’に関わらず、$k_i(+)k_i = 0$が成立することになる。）

バーナム暗号法は鍵が独立したランダムビット列であれば、平文に対して暗号文はランダムビット列となる。メッセージ長と同じ長さのランダムビット系列を関係者以外には分からないよう生成し、かつ送受信者間で共有し合うことができれば、安全な暗号通信を行うことができる。バーナム暗号法においては安全上、キーストリームを使い捨てにすることによって、暗号強度を保っているため、キーストリームの長さは、メッセージ長よりも長くなくてはならない。このキーストリームに真の物理的ランダムビット列を用いた場合、このシステムは解析が不可能な唯一の暗号法となる。しかし、超機密データを通信する場合を除き、実際問題として平文の量と同じ量のキーストリームを別に送信先に送るのは非現実的であり、鍵系列の保管にも問題がある。

【００２７】そこで実用上、ランダムなビット列（擬似ランダムビット列）を適当な長さのＳｅｅｄから生成し、それをバーナム暗号法に適用するのが一般的である。そのため通信者以外の第三者から見て、解読が不能なビット列であり、かつ通信者同士は共通のキーストリームを生成する手法を共有していなくてはならない。暗号文は、実際には第三者からの解読の危機にさらされていることを考慮に入れる必要がある。そのため擬似ランダムビット列生成器を構築するためには、以下の３種類の暗号解読攻撃法を解決しなくてはならない。

【００２８】

１．暗号文のみによる攻撃(ciphertext-only attack)

２．既知平文攻撃(known-plaintext attack)

３．選択平文攻撃(chosen-plaintext attack)

１．は最も一般的な解読法であり、暗号解読者は、暗号化アルゴリズムや平文の言語、通信文の話題（頻度の多い語句）などを知っているかも知れないが、基本的には暗号文からのみ秘密の平文や鍵を決定しなければならない。また２．では、暗号解読者はいくつかの暗号文と平文のペアを知っており、その知識を利用して秘密の鍵を決定し、任意の暗号文に対応した平文を決定する。３．では、暗号解読者が選んだ平文を正規の送信者に暗号化させ、その平文に対応した暗号文を手に入れることができる状況での解読である。これは、暗号解読者にとって最も好ましい状況である。

【００２９】ところで、すべての暗号は実際には多くの時間や資源を用いれば、原理的に解読されてしまう。従って、現実的な計算量で解読できるかどうかが、暗号の安全性を議論する上で重要なポイントであり、現代暗号研究の関心事の一つである。現実的に利用可能な資源と最良の解読アルゴリズムを用いても妥当な時間内に解読できなければ、その暗号は計算量的に安全(computationaly secure)、または強い(strong)と呼べる。

【００３０】このことから、擬似ランダムビット列生成器の構築には、一方向性関数の性質を以て前述の３つの攻撃法に対処しなくてはならない。つまり、Ｓｅｅｄよりキーストリームの生成は比較的容易ではあるが、キーストリームからＳｅｅｄを計算することは困難でなくてはならない。本例の擬似ランダムビット列生成器を使用する通信システムでは、図６に示すような手順で暗号通信を行うことにより、直接送信データの暗号化に使用されるＳｅｅｄを送ることなく、攻撃に強い暗号通信が実現できる。図６では選択データの送信は説明しないが、予備Ｓｅｅｄの送信と同様に実現できる。

【００３１】図６では、まず、ステップＳ１で周期が全Ｓｅｅｄビットを越えるように、新規の予備Ｓｅｅｄをセットする。ステップＳ２で全Ｓｅｅｄビットを作成してセットし、ステップＳ３で送信データの先頭位置に、送信側の擬似ランダムビット列生成器の疑似ランダムビット列で暗号化されたデータが、受信側で復号された時に送信側の予備Ｓｅｅｄとなるように計算されたデータを付加して、送信データを送る。尚、受信側のＳｅｅｄは最新の送信時に送信側から送った予備Ｓｅｅｄに基づいて作成されたＳｅｅｄなっているとする。初めての通信相手には双方に秘密裏に最初の受信時の予備Ｓｅｅｄを配送するようにするのが好ましい。

【００３２】受信側では、ステップＳ４で先頭位置の新規の予備Ｓｅｅｄを復号し、その復号された予備Ｓｅｅｄをセットすると共に、送信相手に対応して次の受信時に使用するために記憶する。次に、ステップＳ５で複合された予備Ｓｅｅｄから全Ｓｅｅｄビットを作成してセットし、ステップＳ６で続く受信データを復号する。

尚、上記例では時間ｔの同期については述べなかったが、時間ｔも暗号化して送ることにより、より攻撃に強い暗号通信が実現できる。また、上記暗号通信では、秘匿性が高い場合に注目した方式を提案したが、構内通信のように秘匿性が多少低い場合には、単にＳｅｅｄや予備Ｓｅｅｄやせん選択データをそのまま、あるいは簡単に暗号化して、送受信側で通報する方式にも本擬似ランダムビット列生成器は有用である。

【００３３】

【発明の効果】本発明により、従来の複数のフィードバックレジスタを用いた擬似ランダムビット列生成器の欠点であった短い周期性を改善しながら、複数のフィードバックレジスタを用いた擬似ランダムビット列生成器の簡素な回路構成と安全性の尊重を目的とした、擬似ランダムビット列生成器及びそれを使用する暗号通信方法を

提供できる。

【図面の簡単な説明】

【図１】本実施の形態の基本擬似ランダムビット列生成器の構成例を示す図である。

【図２】本実施の形態の周期性を改善した擬似ランダムビット列生成器の構成例を示す図である。

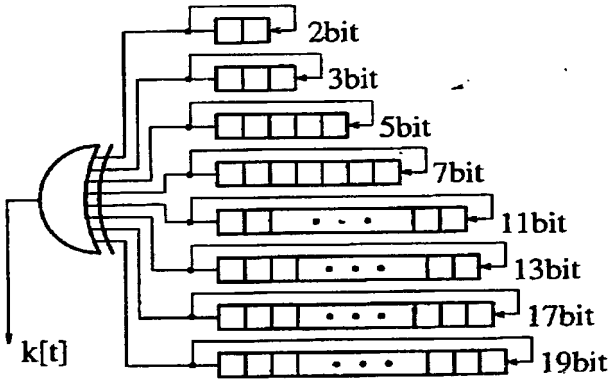
【図３】本実施の形態の秘匿性を改善した擬似ランダムビット列生成器の構成の一例を示す図である。

＊【図４】本実施の形態の秘匿性を改善した擬似ランダムビット列生成器の構成の他例を示す図である。

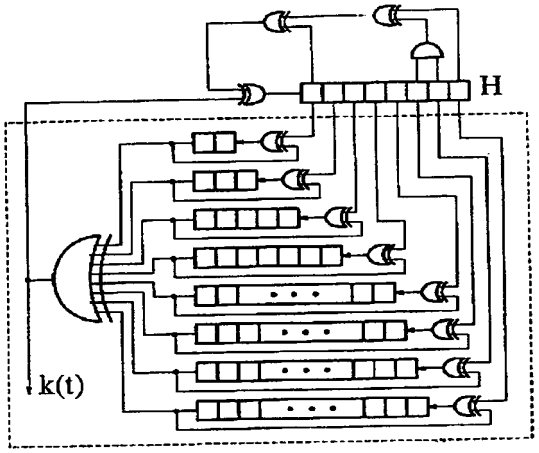
【図５】本実施の形態のバーナム暗号法を説明する図である。

【図６】本実施の形態の擬似ランダムビット列生成器を使用した暗号通信システムの動作手順例を示すフローチャートである。

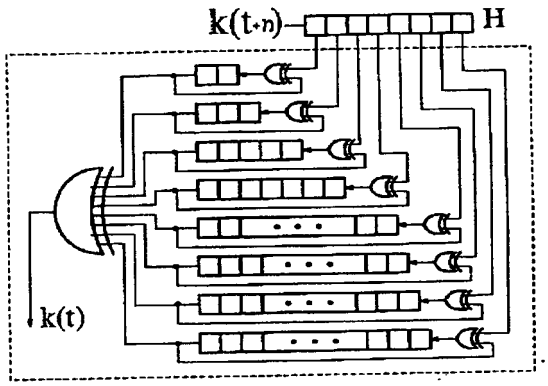
【図１】



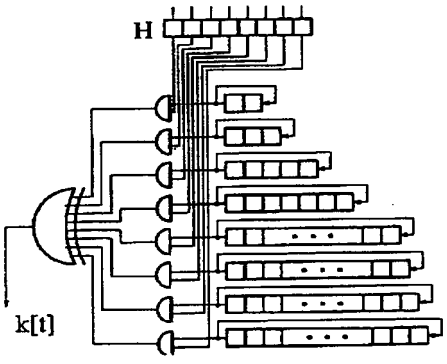
【図２】



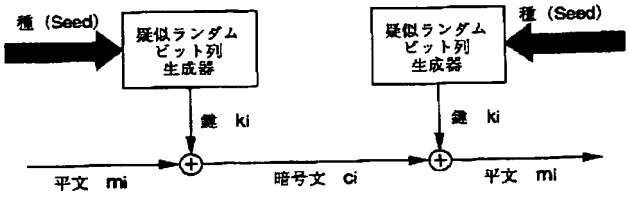
【図３】



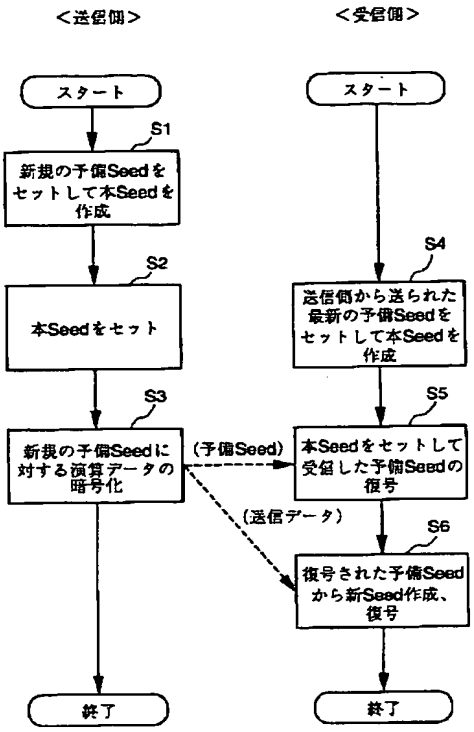
【図４】



【図５】



【図６】


<送信側>
<受信側>
スタート
スタート
S1
新規の予備Seedをセットして本Seedを作成
S2
本Seedをセット
S4
送信側から送られた最新の予備Seedをセットして本Seedを作成
S3
S5
新規の予備Seedに対する演算データの暗号化
(予備Seed)
本Seedをセットして受信した予備Seedの復号
(送信データ)
S6
復号された予備Seedから新Seed作成、復号
終了
終了